Aula 09

Firewall

(Configuração)

Prof. Roitier Campos Gonçalves

O que filtrar?

Duas abordagens:

- Política padrão DROP e regras específicas para os serviços permitidos;
- Política padrão ACCEPT e regras para bloquear serviços específicos.

Em geral, a configuração de um firewall envolve três passos:

- Decidir o que vai ser filtrado;
- Carregar os módulos do kernel necessários para as tarefas a serem feitas;
- Criar as regras e os scripts para carregá-las no kernel.

Políticas de firewall

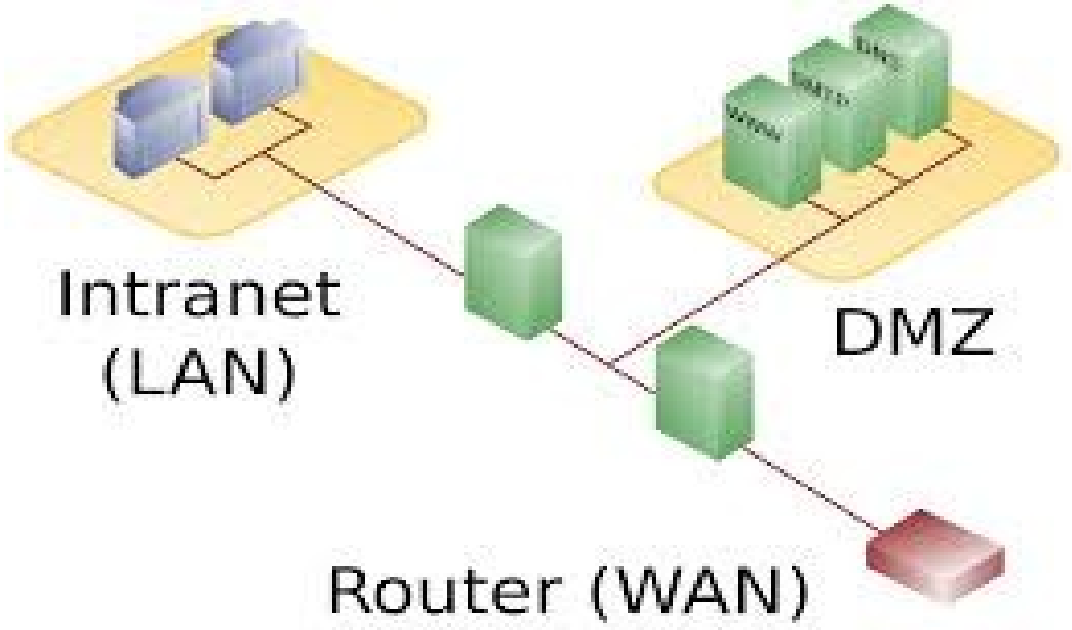
A decisão sobre o que filtrar vai depender da rede ou máquina que se deseja proteger. Cada cenário exige uma configuração de firewall própria. No entanto, podemos ter duas aborda- gens básicas ao criar um firewall.

Em geral esses firewalls são mais restritivos na filtragem de pacotes. Outros firewalls seguem o princípio oposto: deixam passar qualquer pacote, e as regras são criadas para bloqueio de determinados tipos de pacote.

A escolha por uma ou outra abordagem vai depender do que se deseja proteger e da política de segurança adotada pela instituição. Em geral os firewalls que protegem intranets são do primeiro tipo, enquanto que o segundo tipo é utilizado em roteadores de borda para conter determinados ataques e/ou worms.

DMZ

Em algumas situações, também é desejável oferecer alguns serviços para a internet e, ao mesmo tempo, proteger a intranet. Nesses casos é comum a criação das chamadas zonas desmilitarizadas ou DMZ. Uma DMZ é uma sub-rede, na qual são colocadas as máquinas que oferecem serviços para a internet, como servidores web e de e-mail. Ao se configurar um firewall com uma DMZ, o administrador cria regras específicas de acesso para a DMZ e para a intranet.



Módulos do kernel

Principais módulos do netfilter e suas funções:

- ip_tables: habilita o suporte ao netfilter;
- iptables_filter: habilita o suporte à tabela filter;
- iptables_mangle: habilita o suporte à tabela mangle;
- iptables_nat: habilita o suporte à tabela NAT;
- ip_conntrack: habilita o suporte ao reconhecimento de conexões;
- ip_conntrack_ftp: habilita o suporte ao reconhecimento das conexões do FTP ativo (conexões RELATED);
- ipt_state: habilita a permissão para regras baseadas no estado da conexão;
- ipt_LOG: habilita o suporte ao alvo LOG (veja as tabelas de alvos no item seguinte);
- ipt_REJECT: habilita o suporte ao alvo REJECT.

Manipulação de regras

- Sintaxe para criação ou remoção de regras:

  # iptables [-t TABLE] -[AID] CHAIN [N] MATCH -j TARGET

- Use “!” para negar uma opção:

  # iptables -A INPUT -i eth0 ! -s 192.168.0.1 –j DROP

- foi criada uma **chain** para tratar apenas de pacotes ICMP, e essa regra foi chamada de ICMP_FILTER.

  # iptables -A ICMP_FILTER -s 192.168.1.1 -j RETURN

- É possível ter, então, uma regra na chain FORWARD do tipo:

  # iptables -A FORWARD -p icmp -j ICMP_FILTER

- Por exemplo, para que os pacotes com origem em 192.168.1.1 retornem à chain FORWARD, basta criar a regra:

  # iptables -A ICMP_FILTER -s 192.168.1.1 -j RETURN

- “Dropa” (DROP) tudo que chega ao firewall com destino ao host 192.168.0.3:

  # iptables -A FORWARD -d 192.168.0.3/32 -j DROP

- Remove a regra anterior:

  # iptables -D FORWARD -d 192.168.0.3/32 -j DROP

- Bloqueia a porta 23 da máquina local para acessos vindos pela interface eth0:

  # iptables -A INPUT -i eth0 -p tcp --dport 23 -j REJECT

- “Loga” (LOG) tentativas de acesso à porta 161 UDP vindas de fora da rede 192.168.0.0/24, limitando o número de match para não encher rapidamente o log:

  # iptables -A FORWARD -p udp --dport 161 ! -s 192.168.0.0/24 -j LOG --limit 1/second

Listagem de regras

Sintaxe

- # iptables -L [CHAIN] [-t table]

Exemplos:

- # iptables –L - Mostra todas as chains da tabela filter:
- # iptables -L -t mangle - Mostra todas as chains da tabela mangle:
- # iptables -L FORWARD -t filter - Mostra a chain FORWARD da tabela filter:

Para listar o conteúdo de uma chain, basta utilizar o comando:

- iptables -L [CHAIN] [-t table]

Manipulação de chains

Ajuste da política padrão de uma chain (o que fazer caso nenhuma regra se aplique ao pacote):

- # iptables -t filter -P FORWARD DROP

Criar e remover chains:

- # iptables -t filter -N ou -X servicos_tcp

Utilizar chains de usuário:

- # iptables -A INPUT -p tcp --dport 80 -j servicos_tcp

Limpar chains:

- # iptables -t table -F <chain>

Habilitando o repasse de pacotes

Por padrão, o Linux não faz o repasse de pacotes entre suas interfaces, ou seja, ele não atua como um roteador. Quando construímos um firewall para uma rede, é necessário que o sistema seja capaz de encaminhar pacotes vindos de uma rede para outra. Para isso, é necessário habilitar essa função, chamada de IP forwarding. Para habilitá-la, é necessário mudar o valor do arquivo /proc/sys/net/ipv4/ip_forward para 1:

```
# echo 1 > /proc/sys/net/ipv4/ip_forward
```

Automatizando o Firewall